AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2020-25223

Unauthentifizierte Remote-Code-Execution im Sophos SG UTM WebAdmin.

Ein nicht authentifizierter Angreifer aus dem Netz kann über das WebAdmin-Interface der Sophos SG UTM beliebige Betriebssystembefehle mit Root-Rechten ausführen und damit die gesamte Firewall übernehmen. Ursache ist eine Befehls-Injektion über den Session-Identifier (SID), der vom confd-Backend ungeprüft verarbeitet wird. Die Schwachstelle steht seit März 2022 im CISA-KEV-Katalog der aktiv ausgenutzten Lücken, ein öffentliches Exploit-Modul existiert.

Geschäftsrisiko: Vollständige Übernahme der Perimeter-Firewall mit Root-Rechten – der Angreifer kann Regeln manipulieren, den Datenverkehr mitlesen oder umleiten, sich dauerhaft einnisten und ins interne Netz vordringen. Das birgt das Potenzial für Datenabfluss, Betriebsunterbrechung und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

9,8 / 10

KRITISCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | Hoch | Kritisch

`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H` – aus dem Netz, ohne Anmeldung, ohne Zutun – ein Angreifer führt beliebige Befehle mit Root-Rechten auf der Firewall aus. Vertraulichkeit, Integrität und Verfügbarkeit sind vollständig kompromittiert. CVSS 2.0 bewertet die Lücke mit dem Höchstwert 10,0.

AUSGENUTZT SEIT
25. März 2022 (CISA KEV)

BETROFFEN
SG UTM < 9.511 MR11
SG UTM 9.6 < 9.607 MR7
SG UTM 9.7 < 9.705 MR5

HANDLUNGSBEDARF
Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad (3.1)

Unauth RCE
als Root, ohne Anmeldung

Aktiv
ausgenutzt · CISA KEV (seit 25.03.2022)

CWE-78
OS-Command-Injection

Die Ursache: Das WebAdmin-Interface prüft den in einer Anfrage übergebenen **Session-Identifier (SID)** nicht ausreichend, bevor er an den Backend-Dienst `confd` weitergereicht wird. Dieser liest den SID aus dem Sessions-Verzeichnis `/var/confd/var/sessions` – ein **nicht authentifizierter** Angreifer kann den SID durch einen Shell-Befehl ersetzen, der daraufhin mit **Root-Rechten** ausgeführt wird. So wird die Authentifizierung umgangen und beliebiger Code auf der Appliance ausgeführt.

ANGRIFFSKETTE

01
WebAdmin exponiert – das Verwaltungs-Interface der SG UTM ist über das WAN erreichbar

02
SID manipulieren – in einer unauthentifizierten Anfrage wird statt einer gültigen Session-ID ein Shell-Befehl übergeben

03
confd führt aus – der Backend-Dienst verarbeitet den SID ungeprüft, der eingeschleuste Befehl läuft mit Root-Rechten

04
Übernahme – vollständige Kontrolle über die Firewall, Persistenz und Sprungbrett ins interne Netz

Betroffenheit & Fixversionen

SG-UTM-Version	Verwundbar bis	Fixversion (Ziel)
SG UTM 9.5	< 9.511 MR11	9.511 MR11
SG UTM 9.6	< 9.607 MR7	9.607 MR7
SG UTM 9.7	< 9.705 MR5	9.705 MR5

Betroffen ist ausschließlich die klassische Sophos SG UTM (WebAdmin) in den genannten Versionen. Die Fixes wurden am 17. September 2020 veröffentlicht. Nicht betroffen sind die XG-Firewalls mit Sophos Firewall OS (SFOS) – bei ihnen greifen andere Advisories.

Regulatorischer Hinweis: Eine bestätigte Kompromittierung der Firewall oder ein daraus resultierender Abfluss personenbezogener Daten kann eine meldepflichtige Verletzung darstellen – DSGVO unverzüglich (i. d. R. 72 h), NIS-2 nach den für Sie geltenden Fristen. Die Meldung bleibt bei Ihnen; wir unterstützen bei Bewertung und Dokumentation.

ZEITACHSE

18.09.2020
Sophos veröffentlicht Advisory (sophos-sa-20200918) samt Fixes 9.705 MR5 / 9.607 MR7 / 9.511 MR11

18.08.2021
Atredis Partners publiziert technische Deep-Dive-Analyse der Preauth-RCE

2021
Öffentliches Metasploit-Exploit-Modul (SID Command Injection) verfügbar

25.03.2022
CISA nimmt CVE-2020-25223 in den KEV-Katalog auf – aktive Ausnutzung

15.04.2022
KEV-Frist für US-Behörden zum Patchen

Ihr Maßnahmenplan.

In dieser Reihenfolge – WebAdmin vom WAN trennen, patchen, Kompromittierung ausschließen, Zugangsdaten rotieren.

SOFORT	KURZFRISTIG	PARALLEL
WebAdmin vom WAN trennen / patchen	Kompromittierung prüfen (KB-000042965)	Admin-Zugangsdaten rotieren

01 Betroffenheit feststellen

Prüfen, ob eine Sophos SG UTM in einer Version unterhalb `9.511 MR11`, `9.607 MR7` bzw. `9.705 MR5` im Einsatz ist und ob das WebAdmin-Interface über das WAN erreichbar ist.

02 Sofort mitigieren (vor dem Patch)

Das WebAdmin-Interface vom Internet trennen: unter `Management → WebAdmin Settings → WebAdmin Access Configuration → Allowed Networks` ausschließlich interne Netze (z. B. `Internal (LAN)`) zulassen. Von Sophos als Behelfsmaßnahme benannt.

03 Patchen

Auf `9.511 MR11`, `9.607 MR7` oder `9.705 MR5` (bzw. neuer) aktualisieren. Damit ist die Befehls-Injektion geschlossen.

04 Kompromittierung ausschließen

Die von Sophos in KB-000042965 beschriebene Prüfung durchführen und WebAdmin-/Zugriffslogs auf anomale, unauthentifizierte Anfragen sowie unerwartete Prozesse oder Dateien auf der Appliance untersuchen.

05 Zugangsdaten als kompromittiert behandeln

Bei Anzeichen eines Zugriffs alle Admin-Zugangsdaten, Zertifikate und auf der UTM hinterlegten Geheimnisse rotieren – ein Patch macht bereits abgeflossene Geheimnisse oder installierte Hintertüren nicht ungültig.

Kompromittierungs-Indikatoren (IoCs)

AUFFÄLLIGE AKTIVITÄT

Unauthentifizierte Anfragen an das WebAdmin-Interface mit manipuliertem `SID`-Wert

KOMPROMITTIERUNGS-CHECK

Sophos-Anleitung `KB-000042965`
unerwartete Prozesse/Dateien mit Root-Rechten

FOLGEINDIKATOREN

Neue/fremde Admin-Konten, geänderte Regeln
oder ausgehende Verbindungen von der UTM

Zur Einordnung: Die SID-basierte Injektion läuft über reguläre WebAdmin-Anfragen und ist ohne detaillierte Zugriffs-Logs schwer zu erkennen. Der zuverlässigste Weg ist die Sophos-Kompromittierungsprüfung (KB-000042965) in Verbindung mit der Auswertung Ihrer WebAdmin- und Firewall-Logs.

Wichtig: Der Angreifer erlangt Root-Rechte auf der Perimeter-Firewall – dem zentralen Sicherheits- und Übergangspunkt Ihres Netzes. Ein Patch schließt die Lücke, entfernt aber keine bereits eingerichtete Persistenz. Deshalb ist die Kompromittierungsprüfung ebenso wichtig wie das Update; im Zweifel ist die Appliance neu aufzusetzen.

Lassen Sie das von unseren Experten prüfen.

Drei Bausteine, die genau auf diese Schwachstelle einzahlen – vom schnellen Exposure-Check bis zur laufenden Absicherung.

Cyber Defense Center

24/7-SOC aus München: Unauthentifizierte WebAdmin-Anfragen mit manipuliertem SID und daraus resultierende Root-Aktivität auf der UTM fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden erreichbare, ungepatchte SG-UTM-WebAdmin-Instanzen über Ihren gesamten Perimeter – bevor Angreifer sie finden – und priorisieren nach realer Ausnutzung.

Incident-Response-Retainer

Bei Verdacht auf einen bereits erfolgten Zugriff übernimmt unser IR-Team Forensik und Eindämmung – mit vertraglich zugesicherter Reaktionszeit.

SO GEHEN WIR VOR

01 Exposure-Check

Wir prüfen, ob Ihre SG UTM-Systeme verwundbar konfiguriert und exponiert sind.

02 Sofortmaßnahmen begleiten

Mitigation und Patch-Fahrplan gemeinsam mit Ihrem Team umgesetzt.

03 Absichern & überwachen

Threat Hunting auf die IoCs, danach laufendes Monitoring und IR-Bereitschaft – 24/7, wenn Ihr Team das nicht selbst leisten kann.

Empfehlung für die Geschäftsleitung

- WebAdmin heute vom Internet trennen (Allowed Networks auf interne Netze beschränken); Patch auf die MR-Fixversion unverzüglich einplanen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – nach Sophos-Anleitung KB-000042965 und anhand der Logs, dokumentiert für eine etwaige Meldung.
- Bei Kompromittierungsverdacht Admin-Zugangsdaten und Geheimnisse rotieren lassen und Neuaufsetzen der Appliance erwägen.

Ihr Part · unser Part. Sie behalten die Kontrolle über Konfiguration und Freigaben; wir liefern Analyse, Bewertung und – im Retainer – die Reaktionskette.

Rollen, Eingriffstiefe und SLAs im Erstgespräch (RACI, AVV/TOM auf Anfrage) · Datenhaltung auf Wunsch vollständig in Deutschland · ISO/IEC 27001 (TÜV SÜD) · deutschsprachige Analysten.

Sprechen Sie mit uns, bevor es ein Angreifer tut.

Kostenloses 30-Minuten-Erstgespräch – wir prüfen Ihre Exposure gegenüber CVE-2020-25223 und dem SG UTM-Perimeter.

+49 89 45 24 24-100 · kontakt@argos.security · www.argos.security

Termin buchen

Quellen: Sophos Security Advisory sophos-sa-20200918-sg-webadmin-rce (KB-000042965) · NVD (CVSS 3.1: 9,8 / CVSS 2.0: 10,0, CWE-78) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 25.03.2022, Frist 15.04.2022) · Atredis Partners Deep-Dive · Rapid7 Metasploit (SID Command Injection). Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversion gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.